## REMARKS

Reconsideration and allowance are requested.

The Examiner raises a double patenting objection regarding commonly-assigned U.S. patent application 10/714,520. Applicants have filed herewith a terminal disclaimer to remove this objection, but the terminal disclaimer is not an admission that Applicants agree with the objection.

Applicants note with appreciation the indication of allowable subject matter in claims 9-24 and 33-48 and thank the Examiner for his consideration of the information cited in various information disclosure statements.

Claims 1-8, 25-32, 49, and 50 stand rejected for anticipation under 35 U.S.C. 102 by US Patent 6,820,177 to Poisner. This rejection is respectfully traversed.

To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. *Scripps Clinic & Research Found. v. Genentec, Inc.*, 927 F.2d 1565 (Fed. Cir. 1991). Every limitation contained in the claims must be present in the reference, and if even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Poisner fails to satisfy this rigorous standard.

Poisner protects configuration information (rather than data in general) and discloses mapping at least one range of memory addresses to logic external to the system memory. These memory addresses provide a protected configuration space. This protected configuration space, addressed as part of the system memory space, is redirected to protected configuration hardware external to memory which holds control values, provides control information, and performs

operations that are accessible only to "protected commands." See column 2, lines 13-20. In one embodiment, there is also a non-protected configuration space 142 which is also part of the system memory space. Both the protected and the non-protected configuration spaces map to hardware outside the system memory (logic circuit 120 in Figure 1). Thus, when a particular memory location is addressed via a command on the processor bus 130, control logic 124 determines the appropriate response. For a standard access to data in memory, this merely involves directing the access request to the specified location in the memory. Column 3, lines 57-59. When the memory access request is to a configuration space, the access is redirected as appropriate. Column 3, line 63 to column 4, line 15.

Thus, Poisner presents a system wherein a particular set of memory addresses are mapped to an external piece of hardware containing configuration registers, whereas other "normal" memory addresses are handled in a conventional manner. As such, it will be appreciated that in Poisner there is no security mechanism associated with the memory 140. Instead, some memory addresses 141 and 142 are mapped to logic 120, and it is there that the security protocols are implemented by control logic 124 with respect to data stored in the configuration registers. See column 3, line 51 to column 4, line 15.

Amended claim 1 recites that a plurality of devices are coupled to the device bus, and that each device can issue a memory access request. Furthermore, amended claim 1 introduces a reference to modes to distinguish between "modes" and "domains." In particular, claim 1 incorporates the wording of original claim 2, and now specifies that "at least one of the devices is operable in a plurality of modes, including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain." As explained in the specification at page 4, lines 2 to 3, page 28, line 15, page 30, lines 2 to 3, page

37, lines 15 to 17, page 39, lines 17 to 23, page 47, lines 10 to 13, etc., the secure and non-secure domains are provide a mechanism for handling security at the hardware level.

The non-secure and secure domains effectively establish separate worlds, the non-secure world grouping all hardware and software accessible to non-secure applications that do not require security, and the secure world grouping all hardware and software that is only accessible when executing secure code. These domains are different from modes of operation, which typically are only applicable to certain types of devices such as processors, for example a processor that can operate in either user mode or privileged mode. Such processor modes are discussed throughout the application, see for example, page 28, lines 3-6, Figure 21, the description of Figures 3 and 4 on pages 25 and 26, etc. Within the claimed data processing apparatus operating modes within certain devices such as processors still exist. These operating modes may exist in the non-secure domain and the secure domain. As discussed earlier, a number of different devices can be connected to the device bus, and in the examples described, at least one of them is a processor core (see for example page 24, lines 28 to 31). For this reason, and given the fact that not all such devices will operate in different modes, amended claim 1 recites that "at least one of the devices" is operable in a plurality of modes.

The new language in amended claim 2 adds a further distinction between modes and domains. New claim 2 is directed to one example embodiment where "for said at least one of the devices, the plurality of modes are replicated in the secure domain and the non-secure domain." See, for example, Figures 3 and 21 and their associated descriptions.

In contrast to Poisner's system, security is intrinsic to the memory itself in the rejected claims. As a result, the feature in claim 1, "the memory [is] divided between secure memory for storing secure data and non-secure memory for storing non-secure data," is not disclosed in

Poisner. Only part of Poisner's whole memory space is dedicated as protected or non-protected configuration space; hence, the memory is not "divided between secure memory...and non-secure memory." Moreover, memory 140 is not used "for storing secure data" or "for storing non-secure data," because memory addresses that fall within the range reserved for configuration spaces 141 and 142 are redirected outside the memory. No access occurs in memory in those instances. See column 3, lines 3-9.

This distinction is reinforced by the language in claim 1: "each of the devices [is] operable to issue onto the device bus a memory access request when access to an item of data in the memory is required, each memory access request pertaining to either said secure domain or said non-secure domain." Poisner also lacks these features. Not only are there memory access requests that do not pertain to either the protected or the non-protected configuration space, but also an access to an item of data stored in the memory 140 is by definition not part of the mapped protected/non-protected configuration space 141/142. Because Poisner only operates with respect to the defined configuration spaces 141, 142, and the memory 140 is not accessed when those configuration spaces are addressed, Poisner does not disclose the claimed "partition checking logic" that prevents access to secure memory whenever a memory access request pertains to the non-secure domain. Poisner has no control over accesses to data stored in the memory 140.

In concluding that the present invention is anticipated by Poisner, the Examiner apparently (page 4 of the Office Action) maps the protected and non-protected microcode (items 116 and 114) onto the claimed secure and non-secure domains. From the discussion above, this mapping is not appropriate. But even if one adopted this mapping for the sake of argument, then the secure and non-secure modes are missing. In rejecting claims 2 and 26, the Examiner points

to the protected and non-protected regions and equates the secure and non-secure modes to the protected and non-protected activities referred to in column 3, lines 8-14 of Poisner. But these activities are simply what goes on within protected and non-protected regions which the Examiner equates with secure and non-secure domains. As explained above, and as made clear in the claims, domains and modes are different -- they cannot be mapped to the same thing.

For the above reasons, it is respectfully submitted that the independent claims are patentable over Poisner. In addition, the Examiner's attention is directed to the new language in dependent claim 2. Claim 2 specifies that for at least one of the devices on the bus, the "plurality of modes are replicated in said secure domain and said non-secure domain." See Figure 10 and 12 for a non-limiting, example illustration. This feature also is not disclosed in Poisner.

The application is in condition for allowance. An early notice of same is requested.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100